

WHAT IS CLAIMED IS:

1. A method for establishing a secure channel through an indeterminate number of nodes in a network comprising:
 - enrolling a smart card with a unique key per smart card, the unique key derived from a private key that is assigned and distinctive to systems and a card base of a card issuer, an enrolled smart card containing a stored public entity-identifier and the secret unique key;
 - transacting at a point of entry to the network, the transaction creating a PIN encryption key derived from the smart card unique key and a transaction identifier that uniquely identifies the point of entry and transaction sequence number;
 - communicating the PIN encryption key point-to-point in encrypted form through a plurality of nodes in the network; and
 - recovering the PIN at a card issuer server from the PIN encryption key using the card issuer private key.
2. The method according to Claim 1 further comprising:
 - defining public key values (e, N) that are exclusive to a card issuer system and card base, the key value e being a public exponent and the key value N being a modulus in an RSA (Rivest, Shamir, and Adelman Public Key Cryptosystem) system;
 - defining a private key value d that is exclusive to the card issuer system and card base, the private key value d being a secret RSA private key;
 - computing a secret key u that is unique to the smart card using an equation of the form:
$$u = x^d \pmod{N},$$
where x is an entity-identifier that identifies the smart card and the entity; and
 - storing the secret key u on the smart card with public key values x, e, and N.

3. The method according to Claim 1 further comprising:
receiving at an entity-activated terminal an entity-entered Personal Identification

Number (PIN) and an entity-inserted smart card;
passing the PIN to the smart card;
computing at the smart card an equation of the form:

$$K = u \cdot TSN^H \pmod{N},$$

where K is a keying code, u is a secret key, TSN is a transaction sequence identifier that identifies the terminal and a sequence number for a transaction originating at the terminal, H is a hash of transaction data elements, and N is a modulus in an RSA (Rivest, Shamir, and Adelman Public Key Cryptosystem) system; and

hashing at the smart card the keying code K to form the PIN encryption key KPE according to an equation of the form:

$$KPE = h(K),$$

where h() is a hashing algorithm.

4. The method according to Claim 3 further comprising:

hashing at the smart card the keying code K to form an encryption key according to an encryption definition selected from a triple Data Encryption Standard (3-DES) and an Advanced Encryption Standard (AES).

5. The method according to Claim 3 further comprising:

padding the keying code K with transaction-related data prior to the hash operation h(K).

6. The method according to Claim 3 further comprising:

deriving the PIN encryption key KPE uniquely as a function of the secret key u for each transaction, the encryption key KPE being secure from an adversary because the secret key u is unknown.

7. The method according to Claim 6 further comprising:
maintaining the private key value d as a secret known only to the card issuer as
the only entity capable of decrypting the cryptogram C.

8. The method according to Claim 1 further comprising:
receiving a PIN encryption key KPE at a card issuer server;
computing a hash H of transaction data;
computing an RSA (Rivest, Shamir, and Adelman Public Key Cryptosystem)
system encryption t of a transaction sequence identifier TSN that identifies
a transaction terminal and a sequence number for a transaction originating
at the terminal according to an equation of the form:
$$t = TSN^e \pmod{N},$$

where N is a modulus in an RSA system;
computing a cryptogram quantity C using public data according to an equation of
the form:
$$C = x \cdot t^H \pmod{N},$$

where x is an entity-identifier that identifies the smart card and the entity;
decrypting the cryptogram quantity C using the private key value d that is
exclusive to the card issuer system and card base, the private key value d
being a secret RSA private key, the decryption according to an equation of
the form:
$$K = C^d \pmod{N};$$
 and
decrypting the PIN using the PIN encryption key KPE = h(K) where h() is a
hashing algorithm.

9. The method according to Claim 1 further comprising:
encrypting a PIN at the smart card using perfect forward secrecy based on a
random number generation whereby compromise of persistent secret data
does not jeopardize data security of prior transactions.

10. The method according to Claim 1 further comprising:
receiving at an entity-activated terminal an entity-entered Personal Identification
Number (PIN) and an entity-inserted smart card;
passing the PIN to the smart card;
generating a random number r at the smart card that is unique to a transaction;
computing at the smart card an RSA (Rivest, Shamir, and Adelman Public Key
Cryptosystem) system encryption t according to an equation of the form:
$$t = r^e \pmod{N},$$
where e is the public exponent and N the modulus of the RSA system;
computing at the smart card a hash H of common public transaction data;
computing at the smart card a keying code K and a PIN encryption key KPE
according to equations of the form:
$$K = u \cdot r^H \pmod{N}, \text{ and}$$
$$KPE = h(K),$$
where u is a secret key and H is a hash of transaction data elements, and
sending the PIN encryption key KPE and RSA system encryption t through the
network; and
erasing the random number r.

11. The method according to Claim 10 further comprising:
receiving a PIN encryption key KPE and encryption t at a card issuer server;
computing a hash H of transaction data;
computing a cryptogram quantity C using public data according to an equation of
the form:
$$C = x \cdot t^H \pmod{N},$$
where x is an entity-identifier that identifies the smart card and the entity;
decrypting the cryptogram quantity C using the private key value d that is
exclusive to the card issuer system and card base, the private key value d
being a secret RSA private key, the decryption according to an equation of
the form:
$$K = C^d \pmod{N}; \text{ and}$$

decrypting the PIN using the PIN encryption key $KPE = h(K)$ where $h()$ is a hashing algorithm.

12. The method according to Claim 1 further comprising:
computing at the smart card a hash H of transaction data;
communicating the transaction data hash to a card issuer server;
computing at the card issuer server a hash of transaction data; and
verifying the communicated hash with the server-computed hash for authentication and integrity checking.

13. A data security apparatus comprising:
a smart card capable of establishing a secure channel through an indeterminate number of nodes in a network comprising:
an interface capable of communicating with a card reader and/or writer;
a processor coupled to the interface; and
a memory coupled to the processor that stores a public entity-identifier and a secret unique key derived from a private key that is assigned and distinctive to systems and a card base of a card issuer, the memory further comprising a computable readable program code embodied therein that creates a PIN encryption key derived from the smart card unique key and a transaction identifier that uniquely identifies the point of entry and transaction sequence number.

14. The apparatus according to Claim 13 further comprising:
a secret unique key u stored in the memory with public key values x , e , and N where x is an entity-identifier that identifies the smart card and the entity, a key value e is a public exponent and a key value N is a modulus in an RSA (Rivest, Shamir, and Adelman Public Key Cryptosystem) system, the public key values (e , N) being exclusive to a card issuer system and card base; wherein:

the secret key u is unique to the smart card and computed using an equation of the form:

$$u = x^d \pmod{N},$$

where a private key value d is exclusive to the card issuer system and card base, the private key value d being a secret RSA private key.

15. The apparatus according to Claim 13 wherein the memory further comprises:

- a computable readable program code capable of causing the processor to receive an entity-entered Personal Identification Number (PIN);
- a computable readable program code capable of causing the processor to compute an equation of the form:

$$K = u \cdot TSN^H \pmod{N},$$

where K is a keying code, u is a secret key, TSN is a transaction sequence identifier that identifies the terminal and a sequence number for a transaction originating at the terminal, H is a hash of transaction data elements, and N is a modulus in an RSA (Rivest, Shamir, and Adelman Public Key Cryptosystem) system; and

- a computable readable program code capable of causing the processor to hash the keying code K to form the PIN encryption key KPE according to an equation of the form:

$$KPE = h(K),$$

where h() is a hashing algorithm.

16. The apparatus according to Claim 15 wherein the memory further comprises:

- a computable readable program code capable of causing the processor to hash the keying code K to form an encryption key according to an encryption definition selected from a triple Data Encryption Standard (3-DES) and an Advanced Encryption Standard (AES).

17. The apparatus according to Claim 15 wherein the memory further comprises:

- a computable readable program code capable of causing the processor to pad the keying code K with transaction-related data prior to the hash operation h(K).

18. The apparatus according to Claim 13 wherein the memory further comprises:

- a computable readable program code capable of causing the processor to receive an entity-entered Personal Identification Number (PIN);
- a computable readable program code capable of causing the processor to generate a random number r that is unique to a transaction;
- a computable readable program code capable of causing the processor to compute an RSA (Rivest, Shamir, and Adelman Public Key Cryptosystem) system encryption t according to an equation of the form:

$$t = r^e \pmod{N},$$

where e is the public exponent and N the modulus of the RSA system;

- a computable readable program code capable of causing the processor to compute a hash H of common public transaction data;

- a computable readable program code capable of causing the processor to compute a keying code K and a PIN encryption key KPE according to equations of the form:

$$K = u \cdot r^H \pmod{N}, \text{ and}$$

$$KPE = h(K),$$

where u is a secret key and H is a hash of transaction data elements;

- a computable readable program code capable of causing the processor to send the PIN encryption key KPE and RSA system encryption t through the network; and

- a computable readable program code capable of causing the processor to erase the random number r .

19. The apparatus according to Claim 13 wherein the memory further comprises:

- a computable readable program code capable of causing the processor to hash transaction data elements and communicate the hash point-to-point to a card issuer enabling simultaneous key management and integrity checking.

20. A data security apparatus comprising:
an enrollment system capable of usage for establishing a secure channel through
an indeterminate number of nodes in a network, the enrollment system
comprising:
a communication interface capable of communicating with a writer
configured to accept a smart card;
a processor coupled to the communication interface; and
a memory coupled to the processor and having a computable readable
program code embodied therein capable of causing the processor to
initialize and personalize a smart card with a unique key per smart
card, the unique key derived from a private key that is assigned and
distinctive to systems and a card base of a card issuer.
21. The apparatus according to Claim 20 wherein the memory further
comprises:
a computable readable program code capable of causing the processor to write to
an enrolled smart card a stored public entity-identifier and the secret
unique key.
22. The apparatus according to Claim 20 wherein the memory further
comprises:
a computable readable program code capable of causing the processor to define
public key values (e, N) that are exclusive to a card issuer system and card
base, the key value e being a public exponent and the key value N being a
modulus in an RSA (Rivest, Shamir, and Adelman Public Key
Cryptosystem) system;
a computable readable program code capable of causing the processor to define a
private key value d that is exclusive to the card issuer system and card
base, the private key value d being a secret RSA private key;
a computable readable program code capable of causing the processor to compute
a secret key u that is unique to the smart card using an equation of the
form:

$$u = x^d \pmod{N},$$

where x is an entity-identifier that identifies the smart card and the entity;
and

a computable readable program code capable of causing the processor to store the
secret key u on the smart card with public key values x, e, and N.

23. A data security apparatus comprising:

a card issuer server capable of usage for establishing a secure channel through an
indeterminate number of nodes in a network, the card issuer server
comprising:
a communication interface capable of communicating with the network;
a processor coupled to the communication interface; and
a memory coupled to the processor and having a computable readable
program code embodied therein capable of causing the processor to
recover a Personal Identification Number (PIN) from a transaction
PIN encryption key received via the network using a card issuer
private key, the transaction PIN encryption key being derived from
a smart card unique key initialized and personalized to the smart
card and derived from the card issuer private key, and a transaction
identifier that uniquely identifies the point of entry and transaction
sequence number.

24. The apparatus according to Claim 23 wherein:

the smart card unique key is a secret key u that is unique to the smart card and is
computed by a card enrollment system using an equation of the form:

$$u = x^d \pmod{N},$$

where x is an entity-identifier that identifies the smart card and the entity;
a private key value d is a secret RSA private key, and key value N is a
modulus in an RSA (Rivest, Shamir, and Adelman Public Key
Cryptosystem) system, the key values d and N being exclusive to a card
issuer system and card base.

25. The apparatus according to Claim 23 wherein the memory further comprises:

a computable readable program code capable of causing the processor to receive a PIN encryption key KPE at a card enrollment server;

a computable readable program code capable of causing the processor to compute a hash H of transaction data;

a computable readable program code capable of causing the processor to compute an RSA (Rivest, Shamir, and Adelman Public Key Cryptosystem) system encryption t of a transaction sequence identifier TSN that identifies a transaction terminal and a sequence number for a transaction originating at the terminal according to an equation of the form:

$$t = TSN^e \pmod{N};$$

where N is a modulus in an RSA system;

a computable readable program code capable of causing the processor to compute a cryptogram quantity C using public data according to an equation of the form:

$$C = x \cdot t^H \pmod{N},$$

where x is an entity-identifier that identifies the smart card and the entity;

a computable readable program code capable of causing the processor to decrypt the cryptogram quantity C using the private key value d that is exclusive to the card issuer system and card base, the private key value d being a secret RSA private key, the decryption according to an equation of the form:

$$K = C^d \pmod{N}; \text{ and}$$

a computable readable program code capable of causing the processor to decrypt the PIN using the PIN encryption key KPE = h(K) where h() is a hashing algorithm.

26. The apparatus according to Claim 23 wherein the memory further comprises:

- a computable readable program code capable of causing the processor to receive a PIN encryption key KPE and encryption t;
- a computable readable program code capable of causing the processor to compute a hash H of transaction data;
- a computable readable program code capable of causing the processor to compute a cryptogram quantity C using public data according to an equation of the form:

$$C = x \cdot t^H \pmod{N},$$

where x is an entity-identifier that identifies the smart card and the entity; a computable readable program code capable of causing the processor to decrypt the cryptogram quantity C using the private key value d that is exclusive to the card issuer system and card base, the private key value d being a secret RSA private key, the decryption according to an equation of the form:

$$K = C^d \pmod{N}; \text{ and}$$

a computable readable program code capable of causing the processor to decrypt the PIN using the PIN encryption key KPE = h(K) where h() is a hashing algorithm.

27. The apparatus according to Claim 23 wherein the memory further comprises:

a computable readable program code capable of causing the processor to hash transaction data elements and compare the hash from a hash received point-to-point from a smart card enabling simultaneous key management and integrity checking.

28. A transaction system comprising:

a network;
a plurality of servers and/or hosts mutually coupling to the network;
a plurality of terminals coupled to the servers and/or hosts via the network and available for transacting;

a plurality of smart cards enrolled in the transaction system and capable of insertion into the terminals and transacting via the servers; and a plurality of processors distributed among the smart cards, the servers, and/or the terminals, at least one of the processors being capable of establishing a secure channel through an indeterminate number of nodes in the network by creating, communicating, and decrypting a PIN encryption key derived from a smart card unique key and a transaction identifier that uniquely identifies a point of entry terminal and transaction sequence number, the smart card unique key being derived from a private key that is assigned and distinctive to systems and a card base of a card issuer.

29. A transaction system comprising:

a network;
a plurality of servers and/or hosts mutually coupling to the network;
a plurality of terminals coupled to the servers and/or hosts via the network and available for transacting;
a plurality of smart cards enrolled in the transaction system and capable of insertion into the terminals and transacting via the servers; and a plurality of processors distributed among the smart cards, the servers, and/or the terminals, at least one of the processors being capable of establishing a secure channel through an indeterminate number of nodes in the network by creating, communicating, and decrypting a PIN encryption key derived from a smart card unique key and a hash of transaction data elements, enabling simultaneous key management and integrity checking.

30. A transaction system capable of establishing a secure channel through an indeterminate number of nodes in a network comprising:

means for enrolling a smart card with a unique key per smart card, the unique key being derived from a private key that is assigned and distinctive to systems and a card base of a card issuer, an enrolled smart card containing a stored public entity-identifier and the secret unique key;
means for transacting at a point of entry to the network, the transaction creating a PIN encryption key derived from the smart card unique key and a

transaction identifier that uniquely identifies the point of entry and transaction sequence number;
means for communicating the PIN encryption key point-to-point in encrypted form through a plurality of nodes in the network; and
means for recovering the PIN at a card issuer server from the PIN encryption key using the card issuer private key.